As of July19, 2012

Statement of Work

For

Network Operations Center Support Services

HSBP1013A00006
Attachment 1

As of July19, 2012

Table of Contents

1 BACKGROUND

The Department of Homeland Security (DHS) has designated Customs and Border Protection (CBP) as the Executive Agent for DHS OneNet; the departments interconnected Wide Area Network (WAN). DHS OneNet enables the sharing of information across DHS components, to include shared Internet, Intranet, and Extranet services.

The Network Security Operations (NSO) branch, within CBPs, Office of Information and Technology (OIT), is responsible for the end-to-end operations and management of the DHS OneNet and is the Enterprise Network Manager. The Network Operations Center (NOC) currently uses the support of the Network service providers (Verizon and AT&T) and other Contractors to provide OneNet service requirements.

The NOC is a 24 hour a day, seven days a week, 365 days per year (24x7x365) place of operations that provides network operations support, problem identification, troubleshooting, and maintenance for CBP Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN) (DHS OneNet). The NOC is the focal point for network troubleshooting, updating, router and domain name management, and coordination with affiliated networks. The NOC is responsible for providing network fault monitoring, network utilization, network availability, problem tracking and escalation, problem reports and documentation.

The Primary NOC is located in Springfield, Virginia and Secondary NOC is located in Orlando, Florida, and staffed as active/active operations centers. The active/active operation provides for increased situational awareness, increased DHS/CBP OneNet availability, and the staffing to ensure continuity of operations should something happen to the other location.

The network environment, major types of equipment, consist of core and edge Routers, Switches, and Firewalls. (b) (7)(E) [redacted]. The NOC is responsible for providing support to approximately 1,800 offices throughout the world that access CBP LAN, MAN and WAN "OneNet".

Generally the NOC is comprised of four teams rolled under Network Operations and Network Sustainment:

<u>Network Operations</u>:

- Network Command, Control &Communication Center
- Network and Firewall Operations Support

<u>Network Sustainment:</u>

- Network Management and Tools Team
- Change and Configuration Management

These teams support the NOCs located in Springfield, Virginia and Orlando, Florida. In addition, these teams provide tier I, II, and III support to the NOC's service providers Verizon and AT&T.

The NOC, through the Network Command and Control Center, is responsible for the day-to-day monitoring, reporting, troubleshooting, escalating, and coordinating of events related to network communications. Activities impacting the NOC may include: (1) loss of connectivity, (2) slow-downs or latency, (3) scheduled or unscheduled outages, and (4) maintenance or upgrades. NCCC is staffed 24x7x365 with three shifts of mid to senior level technicians. Shift turnover is conducted between each shift and includes a comprehensive list of open events, scheduled/upcoming changes and other "critical" items.

Network Command and Control Center (NCCC). Aligned with the NCCC is a team of Tier II staff that provides remediation and resolution to escalated network issues. This staff is responsible for the day-to-day operations and management of the DHS/CBP LAN, MAN and WAN OneNet and legacy DHS Communications Network (DCN). In addition, they are responsible for maintaining, managing, optimizing and troubleshooting all routing and routing protocols along with troubleshooting any connectivity, latency or unavailability issues that are not related to an actual failure in network service provided communications.

Network and Firewall Operations Support. Additional Tier II support is provided by the NOC Network and Firewall Operations Support Team to implement approved changes to all policy and enforcement rules on firewalls in response to (b) (7)(E)) change requests. The team troubleshoots and resolves all firewall related issues. This team closely coordinates with the Security Operations Center in order to streamline the implementation of network security of the LAN, MAN and WAN environments.

Network Management and Tools. The Network Management and Tools Team (NMTT) is responsible for all aspects of communications network monitoring within NOCs areas of responsibility. The NMTT proactively analyzes network traffic statistics to determine possible points of failure and recommends modifications to existing configurations to avoid unscheduled outages. The NMTT engages with the other NOC teams to mitigate and resolve all detected issues.

The NMTT is responsible for running daily, weekly, monthly and ad-hoc reports for inclusion in briefings to Senior Management. The NMTT provides the NOC Daily Wake-Up calls, which is a daily conference call with other DHS Agencies where upcoming changes or other items of interest are discussed.

The NMTT is the primary group responsible for ensuring that the Managed Service Provider (MSP) Service Level Objectives/Service Level Agreements (SLOs/SLAs) are maintained through regular meetings and reviewing reported availability statistics. The NMTT tracks "chronic" or recurring problems and escalates them within the MSP's Management Chain. These problems are tracked, documented and often result in a reduced monthly cost or refund. The NMTT ensures that network switch and router configurations are kept current (b) (7)(E)

The NMTT is made up of network analysts that have operational management responsibility of all IP address assignments. These members provide quality assurance on vendor installed routers, provide tier III Internet Protocol (IP) support to NOC technicians and ensure IP configurations are accurately documented.

The network service providers, Verizon and AT&T, provide the following services to the DHS/CBP NOC:

- IP WAN Services
- Internet Access Services
- Remote access services
- Out of Band Management
- Private Line Services
- Voice Over Internet Protocol (VOIP) Transport
- Connectivity to Non-DHS Networks
- Network Operations and Management
- Coordination with the Security Operations Center for Incident Response

Change and Configuration Management. The Change and Configuration Management team within the NOC is the group responsible for all approved Network or Infrastructure changes proposed in support of the NOC and its Mission. This team provides a central point of coordination for all NOC-initiated changes to Production network systems. This team also provides Quality Control and Compliance Control of Change Records or Requests for Changes initiated by the NOC or the teams within the NOC. This team develops standard Change Request templates and supporting documents necessary for successful review of proposed changes at the various Change Control Boards that govern all IT changes within CBP, DHS, and DHS components. The Configuration Management “arm” of this team is responsible for ensuring that network device configurations are kept up-to-date in the approved CMDB (Configuration Management Database) tool. This team is responsible for ensuring that stored or archived configuration repositories are routinely inspected and audited to ensure the validity of the data.

2 SCOPE

The Primary and Secondary NOCs are a 24x7x365 center that operates in the confines of a secure facility, organized, staffed, and equipped to manage Network Operations and Maintenance (O&M) functions that have relevance across an enterprise. The Contractor shall provide for network operations support services to DHS OneNet, CBP LAN, and Homeland Security Data Network (HSDN).The Contractor shall provide personnel to assist in performing Information Systems Security Officer (ISSO) functions in support of the Certification & Accreditation (C&A) process at CBP. The Contractor shall support virtual private networking (VPN) solutions and remote access services support, access control, and identity management tasks. The Secondary NOC must provide equivalent services to support the functions being performed at the Primary NOC. The Contractor shall provide trained, qualified, and cleared staff to support these functions. The Contractor will be held accountable for the SLOs outlined in each of the Task Orders.

3 APPLICABLE DOCUMENTS

Contractors shall control and safeguard For Official Use Only (FOUO) information in accordance with DHS Directive (MD 11042.1) “Safeguarding Sensitive but Unclassified (FOUO) Information" dated January 6, 2005.

All Contractor personnel should be familiar with the CBP Security Policy and Procedures Handbook (HB1400-02B), August 13, 2009, Volume IV, Chapter 13, Safeguarding Sensitive But Unclassified (FOUO) Information.

All services provided under this Blanket Purchase Agreement (BPA) shall be compliant with DHS Information Security Policy, identified in MD4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook.

All internal NOC processes and procedures are based on widely accepted industry standard best practices and customized to meet specific DHS/CBP requirements. These documents include escalation procedures, standard operating procedures (SOP), and troubleshooting techniques.

Specific DHS/CBP generated documents, policies, and procedures may contain sensitive information and will be made available to the BPA awardee for viewing, but shall not leave CBP facilities, photocopied, or pen copied verbatim while viewing.

National Institute of Standards and Technology Special Publication (NIST SP 800-53) Guide for Information Security Program Assessments

System Reporting Form Standards for Security Categorization of Federal Information and Information Systems (FIPS 199)

All applicable documents will be identified in the individual Task Order.

4 TASKS AND REQUIREMENTS

4.1 Program Management

The Contractor shall manage activities defined in the Task Order in accordance with project management best practices/principles, to include the documentation of requirements, project plans, schedules, risk registers, and mitigation strategies. The Contractor shall perform the following:

- Identify and resolve risks, issues, and dependencies
- Identify internal and external dependencies
- Provide weekly status reports on the project progress
- Provide monthly invoices to include a summary page itemizing costs at the project level
- The Contractor shall conduct a Program Management Review (PMR) monthly and provide a Program Management Report at this meeting.

4.2 Transition

The Contractor shall be prepared to provide a transition period, not to exceed 90 days, in accordance with their transition plan from the incumbent Contractor. The required period is for the transition planning or program execution, associated with meeting the agreed to transition timeline, as directed by Government personnel. This includes the following:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Review of historic data and business processes
- Introduction to Government personnel, programs, and users to the Contractor's team
- Issuance of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance

4.3 Network Operations Center (NOC) Support

The Contractor shall provide a wide range of Network services that may include monitoring and analysis, firewall changes and administration, switch and router monitoring, troubleshooting outages, anomalies, network issues and administration, escalation and reporting, network trouble ticket tracking, mitigation and integration, and Service Delivery and Implementation.

The Contractor shall be required to develop, update and submit for approval to the Government, standard operating procedures (SOPs), Tactics Techniques & Procedures (TTPs) and Operating Instructions (OIs) as required in support of NOC service support.

The following is a list of NOC support services to be performed by the Contractor:

4.3.1 Network Problem Identification, Troubleshooting, and Maintenance

The Contractor is responsible for identifying, diagnosing, defining, performing, and documenting Tier II remedial actions taken to resolve network connectivity issues affecting Data Center systems and services in the production environment. The Contractor shall support this by completing the following in accordance with the applicable documents identified in the Task Order:

- Create a ticket in Remedy as soon as a condition is detected that has a performance impact on network services
- Adhere to established guidelines when assigning severity levels to tickets based on service level impact (i.e., service levels identified in the Task Order)
- In the event of a network problem requiring Tier III support, the NOC Tier II will indicate the presence of network problems through the redistribution of a trouble ticket (via the Remedy Action Request System – the current problem reporting system) to the Tier III Network Engineering support responsibility area.
- Troubleshoot WAN/LAN to isolate the source of problems, resolve all network problems, or refer the problems to the appropriate responsibility area or escalation point.

Network components may include such devices as:

- Cabling
- Modems
- Digital/channel service units
- Concentrators
- Bridges
- Routers
- Switches
- Firewalls
- Fileservers
- Link encryption devices
- Secure frame units
- Gateways and protocol converters
- Specialized appliances or hardware that provide network services (i.e., Domain Name Services/Dynamic Host Configuration Protocol (DNS/DHCP), Proxy Services, and Security Services)

The Contractor shall continuously monitor the Remedy trouble ticket system for new escalated tickets and update at a minimum every hour and when appropriate. All information entered into a ticket must be clear, concise and accurate. Upon receipt of a trouble ticket, the Contractor shall initiate immediate action to clearly define the problem and effect immediate resolution, and document the problem in the trouble ticketing system to effectively track it to satisfactory resolution, or redistribute it to the appropriate group of responsibility for action toward satisfactory resolution.

The Contractor shall conduct an analysis of the system components (listed above) to determine effectiveness and make a recommendation to the Government based upon diagnostic information provided by approved Government sources, to include Government owned network monitoring and management software tools (i.e., HPNa, CA eHealth/LiveHealth, Netcool, NetView, and Tivoli) and future management tools identified in the Task Order.

The Contractor may access the network during the course of troubleshooting problems in order to use diagnostic applications resident in the system. In addition, the Contractor shall be responsible for monitoring all network devices using Government owned network monitoring and management software tools (i.e., HPNa, CA, eHealth/LiveHealth, Netcool, NetView, and Tivoli) currently in place, to include any future additions to the hardware configuration.

The Contractor shall document each step in resolving Remedy tickets as outlined in SOPs. Due to the complex nature of networks, it is possible for the source of a network problem to reside in one or more devices concurrently. As such, the Contractor must perform troubleshooting techniques to isolate the source of the issue diagnose, and resolve or assist in the resolution of network problems.

The Contractor shall participate in /or lead conference calls during mitigation actions of network anomalies.

4.3.2 Network Problem Resolution and Referral

The Contractor shall use Government-approved documented escalation procedures when referring network problems to external support organizations such as the Network Engineering Branch, the Hardware or Solution Vendor or another DHS Component when resolution cannot be achieved by Contractor personnel. If diagnosis or resolution cannot be completed in accordance with the current established escalation policy, the Contractor must escalate the problem to higher authority (i.e., Tier III engineering support) for further action within the organization.

The Contractor shall contact the Government Team Lead or Government Watch Officer when problems are detected in hardware or circuits that are operated, maintained or under warranty by the vendor. The Government shall provide the Contractor with an up-to-date list of vendors, maintenance providers, service providers and other external support organizations; to include an inventory of the components for which they provide support.

4.3.3 Network Availability

The Contractor shall provide continuous network availability monitoring using government provided software. This includes conducting verification and validation of network availability of outage statistics and monitoring the network Quality of Service (QOS) to ensure provisioned services are adequate for specific applications and that these services continue to meet CBP requirements.

4.3.4 Network Trend Analysis

The Contractor shall conduct a network trend analysis to compile daily and/or longer-term reports for various network traffic areas of interest. These reports shall supply both generalized and specific information about targeted areas and must provide useful snapshots of information. These reports shall include but are not limited to daily and weekly reports covering various error conditions, workload (i.e. CPU and memory), and network utilization. Customized trend analysis reports shall be provided based on current monitoring capabilities with emphasis on tools such as CA’s eHealth.

4.3.5 Network Capacity Planning

The Contractor shall perform data collection using government provided monitoring tools (CA’s eHealth) for input to network capacity planning when triggered by a network availability event. The Contractor shall determine bandwidth utilization using network and configuration information against predetermine network availability thresholds .This information must be used to better estimate future requirements based on application, organizational, or technological changes as well as adjustments to provide improved cost/benefit resources.

4.3.6 Network Problem Resolution Procedures, Documentation, and Reporting

The Contractor shall take appropriate action towards problem status documentation, resolution and prevention as required, in accordance with the SOPs identified in the Task Order.

Following the SOP, the Contractor shall provide required information to the impacted organizations of the network issue regarding the status of changes, enhancements, and problem resolution. The Contractor shall complete resolution or referral of all network problems in accordance with the SOP after receiving Remedy Notification.

The Contractor shall manually enter a narrative description in trouble tickets of all information relative to trouble shooting problems to resolution and completion status.

The Contractor shall ensure that all documentation is completed in accordance with the SOP.

4.3.7 Network Installation Support

The Contractor shall install or modify network components and other systems. This may include physical and logical connections with switches, routers, firewalls, link encryption devices, and public/private key hardware/software components. No modifications or changes will be made without an approved Government Change Record, Emergency Change Record, or Emergency Break/Fix Request. The Change Record will be provided by the Government Team Lead, the Government Watch Officer, or the NOC Director.

The Contractor shall implement configuration and change management processes and support tracking and reporting of configuration changes. The primary DHS/CBP NOC keeps the configuration of all DHS/CBP site Nodes.

The Contractor shall update the configuration of the affected system using standard procedures identified in the Task Order, once a configuration change is made to a DHS/CBP Node. The Contractor shall work with the Government Lead to adhere to these standard operating procedures for introducing a scheduled maintenance or network diversity change.

The Contractor shall support troubleshooting network problems by providing technical support associated with new or revised hardware or software installations. The Contractor shall support coordination of new off-network connections including direct links with other agencies as identified in the Task Order.

The Contractor shall provide support in resolving or referring connectivity problems that may occur when DHS Component offices are relocated, to include problems resulting from the installation of new off-network links. The Contractor shall update baseline artifacts to include logical design, as-is drawing, and other baseline documents as needed. Occasional staff travel requirements may occur and will be addressed on a case by case basis.

4.3.8 Network Operations Center (NOC) Communications Area Equipment Access Control

The Government will approve and control access to the NOC Communications Area for Contractor work to be performed.

The Contractor shall assist in establishing and maintaining user access control procedures, checklists, equipment documentation, and diagrams on an annual basis or as defined in the Task Order.

4.3.9 Problem Tracking and Escalation

The Contractor shall be responsible for tracking all network component failures and effecting escalation actions necessary to ensure appropriate vendor support response and within designated time thresholds established, or ensuring that the Network Management Tools (i.e., HPNa, CA eHealth/Live Health, Netcool, NetView, and Tivoli) are configured appropriately. For serious network degradation, the NOC network management tools will be configured with thresholds that will alert NOC technicians of a potential problem and a trouble ticket has to be generated for tracking and troubleshooting purposes. For high bandwidth utilization, the ticket is escalated for further performance and analysis statistics within the NOC. Escalations or recommendations to another functional area will be made to the Government Team Lead.

The Contractor shall ensure that all information relevant to the incident or action (to include log data, error codes, previous troubleshooting steps and/or attempts) are included in the network systems Remedy trouble ticketing system.

4.3.10 Problem Reporting

The Contractor shall complete problem status documentation, management problem briefs, and ticket status reports.

When directed by the Government the Contractor shall coordinate and work directly with the network services providers, alternate support vendors and support groups to identify and recommend network solutions.

The Contractor shall provide daily Network Operations Briefings to discuss outages to the NOC director to ensure that executive leadership has situational awareness of network anomalies and impacts associated with network outages.

4.3.11 Network Fault and Performance Monitoring

The Contractor shall use current management tools to monitor the current network architecture as well as additions and changes to devices and configurations.

The Contractor will have access to the use of a wide assortment of management tools to assist in identifying, analyzing and defining network system problems. These tools include, but are not limited to HPNa, CA eHealth/LiveHealth, Netcool, NetView, Tivoli, Managed Objects and other distributed processing-oriented management tools.

4.3.12 Service Delivery and Implementation (SDI)

The Contractor shall staff the SDI Team to facilitate the service transition of infrastructure and services into the Network Operations Center operational environment. Contractor support shall include validating compliance with agreed upon “hand off” procedures; coordinating implementation of the applicable systems across the DHS and/or CBP WANs and/LANs; receipt and review of all relevant documentation; and drafting and updating network implementation plan.

As new infrastructures, initiatives and/or systems are brought into the operational environment, a “hand-off” from the transferring organization to NOC is performed and acceptance is required before O&M functions commence. The Contractor shall track Network events through Remedy or an equivalent tool, and will manage a NOC Implementation calendar.

The SDI Team will have access to the transferring organization’s document repository when available for project archival records. The SDI team will maintain a SharePoint site which will house Network Transition Checklist documents and all necessary O&M documents.

For informational purposes, the historical positions and functional roles for the SDI team are listed below; however, the Contractor may propose alternate staffing for this team as appropriate to correlate with the Contractor’s technical and management approach to meeting this requirement.

One Team Lead
Two Project Managers (PM)
One Project Coordinator
One NOC Tier 2 Engineer
One Tier 3 network Engineer

It is anticipated that all of the SDI Team positions listed above will represent full-time duties except for the two engineer positions, which may be performed as ancillary duties.

<u>Note: The positions listed above represent functional roles for the SDI team, not labor categories.</u>

<u>Roles and Responsibilities:</u>

SDI Team Lead: Upon notification of a project or task, the SDI Team Lead oversees and assigns SDI PMs to work with the third party PMs throughout the project lifecycle. The SDI Team Lead assists in building the project schedule and determines required resources. Prior to implementation, the SDI Team Lead PM confirms that required documentation is accounted for and the Network Transition Checklist is complete. Upon successful implementation, the SDI Team lead forwards the completed Network Transition Checklist and accompanying documentation to the NOC Director for “hand-off” approval.

SDI Project Managers: Upon notification of upcoming projects and tasks from the Team Lead, PMs will engage third party PMs and offer ENCC input to the Project Schedule. Will monitor the Project Schedule draft process, but will not allocate ENCC resources until the Schedule has been approved. PMs will work with SDI Tier 2 and Tier 3 engineers to determine schedule and scope of work. Will keep other ENCC teams informed of upcoming events, and will coordinate resource requests with appropriate ENCC team leads. PMs will be responsible for coordinating interaction between third party engineers and other ENCC teams when SDI engineer interaction is not required or redundant.

SDI Engineers (Tier 2 and 3): Engineers will serve as primary technical Points of Contact (POCs) for third party engineers. Will perform NOC related tasks as required, serving as the third party engineer's window into the ENCC. Engineers will assist where applicable in design support and will handle all ENCC implementation duties. As needed, additional Tier 2 and Tier 3 ramp-up support will be requested from NOC and Tier 3 team leads. Need for additional resources will be determined in consultation with the SDI PM.

SDI Project Coordinator (PC): PC will assist SDI Team Lead and SDI PM's as required. Will support the team's overall mission with administrative support where required, and will serve as assistant PM on larger scope projects. The SDI PC has the responsibility of maintaining the implementation calendar, while working toward developing an automated version.

4.3.13 Change and Configuration Management Support

The Contractor shall review network change requests (CR) and configuration changes as subject matter experts.

The Contractor shall support Change Control Board (CCB) meetings that directly or indirectly assist in providing CR review services to the CBP network environment and provide advisement to approve, rework, or deny CRs to the appropriate Branch Director and CCB voting members.

The Contractor shall provide justifications and supporting documentation for advisements, provide recommendations for configuration management, and check for compliance to DHS policy, standards, and hardening guidelines.

The Contractor shall review test plans, User Acceptance Tests and recommend upgrades to automated tools to prevent, monitor and assess the status of the network, data centers, and Component level LANs, when applicable.

4.4 Information Systems Security Officer (ISSO)

The Contractor shall provide personnel, as identified in the Task Order, to assist in the performance of ISSO duties in support of the C&A process at the Primary NOC. Assisting the ISSO may include reviewing security solutions and interpretations of security policies as they relate to specific security infrastructure, architectures and information systems (IS’s). The Contractor shall assist the ISSO in performance of the following duties:

- Participate in appropriate actions to certify and accredit each IS
- Notify the Information Systems Security Manager (ISSM) when an assigned system requires accreditation or re-accreditation
- Lead the C&A process of each system supporting the CBP Network
- Provide policy and security advice to systems designers, implementers and operators
- Conduct risk assessments and prepare an appropriate summary of findings for inclusion within the accreditation documentation
- Conduct self-assessments of the CBP major applications and general support systems, which shall include vulnerabilities identified at Contractor/consultant facilities
- Recommend corrective actions for deficiencies found during system self-assessments (NIST 800-26 or NIST 800-53A) reviews and or during any review or monitoring period for the system/application
- Ensure timely Plan of Action & Milestones (POA&Ms) is uploaded and updated in the Trusted Agent Federal Information Security Management Act (FISMA) tool as required
- Draft, review and submit for Government approval all information systems security plans and other C&A artifacts, not including the Security Assessment Report (SAR). These artifacts include but are not limited to the development of the following documents:
    - Privacy Threshold Determination
    - Privacy Impact Assessment (PIA)
    - E-Authentication Determination
    - Controls Testing (Security Test and Evaluation (ST&E)) Plan
    - ST&E Plan Test Results
    - Authorization to Operate (ATO) Authorization Letter
    - Self-Assessment (National Institute of Standards and Technology Special Publication (NIST SP 800-53) Guide for Information Security Program Assessments and System Reporting Form
    - Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) Assessment
    - Risk Assessment
    - System Security Plan
    - Contingency Plan
    - Contingency Plan Test and Test Results
    - ST&ESecurity Assessment Report
    - POA&Ms
- Assist in the investigation of security violations and incidents
- Be knowledgeable on current Federal, National, DHS and CBP standards, policies, requirements and procedures
- Complete/update a NIST SP 800-26 or NIST SP 800-53 review for each major application, LAN(s), or general support system on a yearly basis
- Review and Update System Security Plan annually and when significant security changes occur
- Review, Update, and Develop Interconnection Security Agreement

- Provide support to administer the network monitoring tools for all NOC teams by creating views within the tools to enable the other NOC teams to productively utilize these tools with the optimal configuration and views

5 DELIVERABLES AND DELIVERY SCHEDULE

5.1 Project Management Plan

The Contractor shall develop a Project Management Plan for this effort. In the Project Management Plan the Contractor shall provide the following:

- Detail schedule identifying work activities, deliverables due dates and milestones
- Risk, and any other items impacting performance of this task
- Quality Control
- Transition In/Out Plan
- Other details as defined in the Task Order

5.2 Performance Metrics

The Contractor shall assist in the development of the NSO performance and business metrics for each of the supported tasks relating to the NOC Task Order requirements. These metrics will represent tangible and concise measures of success and will be used to track Contractor progress in meeting the NOC objectives.

5.3 Presentations

The Contractor shall prepare presentations, as requested, covering work described in the Task Order SOW. These presentations shall be prepared in Microsoft Power Point or as otherwise directed by the OTM.

5.4 Standard Operating Procedures (SOPs), Tactics Techniques Procedures (TTPs) and Operating Instructions (OIs)

The Contractor shall maintain and draft (if needed) NOC SOPs, TTPs and OI's. The SOPs, TTPs, and OIs provide the operational basis for the DHS NOC Concept of Operations (ConOps), NOC Memoranda of Agreements and NOC Center to Center Guidelines, and any Memorandum of Agreement between DHS NOC and the Component NOC's. The Contractor shall review these documents and make recommended updates on an annual basis or as required in the Task Order.

5.5 Service Level Objectives

The Contractor shall draft Service Level Objectives (SLO's) between the OneNet NOC and Component NOCs as additional services and/or component services are subscribed to.

5.6 Daily Situational Awareness Brief

The Contractor shall facilitate a daily NOC Enterprise Situational Awareness Brief with the DHS/CBP leadership. This brief will be in Microsoft Power Point and will include all Network Operations events. The government will provide the Contractor with the format of the Daily Situational Awareness Brief at the Task Order award kick-off meeting. In addition the Contractor shall recommend a strategy to automate the situational awareness brief to the leadership and enterprise components.

5.7 Daily Status Report

The Contractor shall facilitate a daily NOC operational conference call with the duty officer, and provide daily status report to support the DHS/CBP NOC operations. The Contractor shall submit NOC input to the agenda and provide updated detailed activity daily by 6:00 A.M. Conference call information shall include any reported Component Network outage, Network event notifications, Network device outages, alerts, Firewall issues, major network configuration changes and bandwidth anomaly in the previous reporting cycle (i.e., last 24 hours, or back to the last Federal business day). This information may be accessed by authorized users to retrieve ad-hoc reports using the CBP/DHS NOC On-Line web portal. The Contractor shall maintain the website, administer users and update continuously to provide real-time information for the daily conference call NOC report. The following is a list of required reports:

- Network infrastructure outage reports
- Network firewall outages/anomaly reports
- Bandwidth anomaly issues
- Network device outages/anomalies
- Top 100 circuit outages/anomalies
- Significant component network issues/anomalies

5.8 Weekly Status Reports (Bandwidth, Ticketing)

The Contractor shall provide a written weekly report that consists of a summary of all NOC activities and reference analysis of NOC performance metrics, track status of network events, by category, tickets, call logs, investigatory cases, network event notifications, issues & risks and actions accomplished for the week. This report shall be prepared by the NOC Project Manager and must be presented to the OTM by noon Wednesday for inclusion into the weekly report CBP Office of Information Technology.

5.9 Monthly Program Review Reports (Bandwidth, Ticketing, Budget, Personnel)

The Contractor shall submit monthly status reports to the OTM, the COR and the Contracting Officer (CO) on the progress made during the respective reporting period in performance of the Task Order work requirements. The report must address work completed during the current period, planned activities, and problems/issues with recommended solutions, anticipated delays, and resources expended. The report must include planned work assignments and desired results for the next reporting period. The reports must be detailed to provide an ongoing record of all support efforts. For each Task Order, the Contractor must provide a budget including cumulative expenditures and balance remaining.

This report must be submitted within 5 calendar days following the end of each month. The report must be delivered in one hard copy and one electronically provided (email) soft copy in a format to be agreed upon with the OTM.

5.10 Briefing/Meeting Minutes

For each briefing/meeting, the Contractor shall provide the essential elements of the relevant subject matter and an agenda. Meeting minutes shall be prepared and presented in a clear, concise and orderly manner. Appropriate briefing tools such as Microsoft Power Point, overhead slides, plotted charts, etc., must be used. Hardcopy handouts of all briefing materials must be made available to all attendees prior to, or at the time of the briefing.

5.11 Kick-Off Meeting/Draft Project Schedule

A Task Order kick-off meeting will be scheduled within 10 days after award. Attendees will include at a minimum: The COR, OTM, Technical Point of Contact(s) (TPOCs), NOC Project Team Leads and the Contractor Program Manager, and Contractor counter parts/key personnel. The Contractor must provide a draft schedule of their plan to meet the requirements as identified in the Task Order SOW. The schedule will be due 10 days after Task Order award. Any changes or adjustments to the approved schedule must be coordinated with the COTR and appropriate OTM.

5.12 After Action Reports

The Contractor shall provide the Government with after action reports regarding troubleshooting efforts and/or resolution actions taken during network event troubleshooting.

5.13 Engineering Change Request (CR) Report

The Contractor shall review network changes being proposed by the Network Architecture and Engineering Division that directly affect the NOC’s areas of responsibility. All changes to the network shall be reviewed for concurrence prior to implementation.

5.14 NOC Certification & Accreditation (C&A) Documentation

The Contractor shall provide systematic procedure documentation for evaluating, describing, testing and authorizing systems prior to or after a system is in operation.

5.15 Activity Service Level Offering Compliance Report

The Contractor shall provide a monthly report to track Service Level compliance with 3rd Party vendors or Service Providers (i.e. Telecommunications Providers).

5.16 Monthly Status Monitoring and Analysis Reports

The Contractor shall provide a monthly report that depicts the “health and well-being” of the overall network to include network bandwidth utilization, error rates, dropped packets, and field site outages.

5.17 Network Trend Analysis Report

The Contractor shall provide a trend analysis report that depicts daily and/or longer-term for spikes of network traffic areas. These reports shall supply both generalized and specific information about government provided targeted area for a specified period of time. These reports shall include but are not limited to daily and weekly reports covering various error conditions, workload (i.e. CPU and memory), and network utilization. Customized trend analysis reports shall be provided based on current monitoring capabilities such as CA’s eHealth.

5.18 Deliverables Table

The work products shall be delivered in accordance with the schedule set forth in each Task Order. The Contractor shall refer to the Task Order for place of and method of delivery to CBP.

See BPA Task Order

6 ACCEPTANCE REQUIREMENTS OF DELIVERABLES

6.1 Quality

The Government reserves the right to reject any deliverable based on defects with respect to completeness correctness, clarity, and consistencies. In the event of a rejection of any deliverable, the CO will notify the Contractor in writing within five (5) business days of the receipt of the deliverable of any deficiencies to be corrected. The Contractor shall have five (5) business days to correct the deficiencies.

General quality measures, as set forth below must be applied to each work product received from the Contractor under the Task Order SOW.

Accuracy – Work products must be accurate in presentation, technical content and adherence to accepted elements of style.

Clarity - Work products must be clear and concise; engineering terms must be used, as appropriate. All diagrams must be easy to understand and be relevant to the supporting narrative.

Conformance to Requirements – All work products must satisfy the requirements of the work request. The product must adhere to CBP System Engineering Lifecycle (SELC) and DHS based templates, standards and directives.

File Editing - All text and diagrammatic files must be editable by the Government.

Format - Work products must be submitted in Microsoft and/or government required application data processing products. The work product format may change from subtask to subtask. Hard copy formats must follow CBP/DHS Directives and must be consistent with similar efforts.

Timeliness - Work products must be submitted on or before the due date specified in the Work Request or submitted in accordance with a later scheduled date determined by the Government.

6.2 Report Formats

All reports must be delivered in softcopy electronic format, unless otherwise identified. Softcopies must be delivered utilizing Microsoft Office file formats. The Contractor must submit all reports electronically to the COR's electronic mail address and other recipients as directed. In the event the system is unavailable or not accessible due to a system malfunction, the Contractor must submit all reports in a typewritten format to be followed simultaneously with an electronically transmitted copy as soon as the electronic mail system becomes available.

7 CONSTRAINTS

7.1 Break/Fix Resolutions

Break/fix resolutions must be consistent with industry best practices, Department principles, Configuration Management (CM), Technical Reference Model, and System Engineering Life Cycle.

7.2 Solutions

Solutions shall be compliant with the Department Enterprise Architecture directives, OneNet architecture, the Federal Information Security Management Act (FISMA) and other applicable federal, Department security, acquisition, IT, and asset management laws, regulations, rules, and policies.

Solutions shall be compliant with Enterprise Network Engineering Services: Governance Technical Reference Model.

7.3 Architecture Review Board

All changes to production shall follow the approved Architecture Review Board (ARB) and Change Management Policy.

7.4 Service Level Objectives

Contractor shall maintain proper levels of staff coverage and skill set to adhere to the Service Level Objectives (SLO) as outlined in each Task Order.

7.5 Tools

The Contractor shall use only Government provided tools identified in each Task Order when diagnosing problems. The Contractor may recommend tools to enhance or replace existing tools.

8 GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

8.1 Government Furnished Equipment

The Government will provide Contractor personnel with work areas equipped with a workstation, and have access to a printer, telephones, and general office supplies.

8.2 Government Furnished Information

- System Life Cycle documentation
- Separation Procedures for Contractor Employees
- Information Systems Security Policies and Procedures documentation to be furnished upon award
- Process Asset documentation
- Technical Reference documentation
- Current CBP LAN and OneNet enterprise architecture documentation
- CBP LAN and OneNet Network, Directory, Messaging, Collaboration, and Engineering Documentation

8.3 Storage and Management of Government Furnished Information

The Contractor shall comply with storage and management of government furnished information in accordance with official policy.

8.4 Government Furnished Tools

HPNa, CA eHealth/LiveHealth, Netcool, NetView, Tivoli, and other distributed processing-oriented management tools identified in the Task Order.

8.5 Access to Government Property and Facilities

The Government will provide access to appropriate resources within the facilities, including, but not limited to: related employees/ vendors/ developers/ consultants, appropriate work space, hardware, software, network connections, test and live data.

9 PLACE OF PERFORMANCE

Work will be performed at the CBP Network Operations Facility located in the Washington, D.C. metropolitan area and Orlando, FL metropolitan area. Addresses and distribution of workforce will be identified in the Task Order.

Pursuant to Disaster Recovery Operation Center (DROC) processes and procedures, in the event of an actual catastrophic failure at the NDC sites, the CBP NOC would operate from a remote location outside of the D.C. metropolitan area. During the annual Disaster Recovery Test the CBP NOC would operate from a remote location within the D.C. metropolitan area.

10 PERIOD OF PERFORMANCE

The BPA will consist of a base period of twelve months from date of award and three one-year option periods. Task Orders can extend up to twelve months after the expiration of the BPA ordering date.

11 SECURITY

The Contractor must comply with administrative, physical and technical security controls to ensure that the Government's security requirements are met. During the course of the BPA, the Contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of work identified in the Task Order.

11.1 Personnel Security Background Data

All personnel employed by the Contractor and/or responsible to the Contractor for work performed hereunder must either currently possess or be able to favorably pass a full field five (5) year background investigation BI) hired as replacement(s) during the term of this BPA. BIs are taking approximately six (6) months from initial acceptance of the security package.

The information must be correct and reviewed by the designated Security Official for completeness. Normally, information requested for a BI consists of SF-85P, "Questionnaire for Public Trust Positions" or SF-86, "Questionnaire for Sensitive Positions (For National Security)" TDF 67-32.5, "U.S. USCS Authorization for Release of Information", FD-258, "Fingerprint Chart" and a Financial Statement. Failure of any Contractor personnel to successfully pass a BI is cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate. This policy also applies to any personnel hired as replacements during the term of the SOW.

The Contractor shall immediately notify the COR of any personnel changes.

The Contractor is responsible for ensuring that Contractor employees separating from the agency complete the appropriate documentation. This requirement covers all Contractor employees who depart while the Task Order SOW is still active (including resignation, termination, etc.) or upon final completion of the Task Order SOW. Failure of a Contractor to properly comply with these requirements must be documented and considered when completing Contractor Performance

Reports.

The Contractor shall submit within ten (10) working days after Task Order award a list containing the full name, social security number, and date of birth of those people who require a BI by CBP, and submit such information and documentation as may be required by the Government to have a BI performed. The information provided must be correct and reviewed by the Contractor for completeness. Failure of any Contractor personnel to pass a BI is cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined. This policy also applies to any personnel hired as replacements during the term of the contract.

The Contractor shall notify the COR and the CO of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers. The Contractor is responsible for the completion and timely submission to the COR of appropriate documentation for all departing Contractor personnel.

In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees (CF-242)", the Contractor is responsible for ensuring that contract employees separating from the agency complete the relevant portions of the CF-242. The Contractor shall notify the COTR and CBP OIT Workforce Management Group (WMG), BI Coordinator of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and reassignments including those to another contract. This requirement covers all Contractor employees who depart while the contract is still active (including resignations, termination, etc) or upon final completion of contracts. Failure of a contract to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports. The Contractor/Program Manager is responsible for the completion and timely submission to the COR of the CF-242 for all departing contract personnel. The Contractor shall provide the following information to OIT WMG at Tel. (703) 921-6237 and FAX (703) 921-6780:

FULL NAME
SOCIAL SECURITY NUMBER
EFFECTIVE DATE
REASON FOR CHANGE

11.2 Contractor Identification

Contractor employees are required to wear Government provided, CBP approved identification badges at all times when working in Government facilities.

Additional Personnel Security Data

The Contractor shall ensure that its personnel use the following format signature on all official e-mails generated by CBP computers:

[Name]
[Position or Professional Title]
[Company Name]
Supporting the XXX Division/Office
US Customs and Border Protection
[Phone]
[FAX]
[Other contract information as desired]

11.3 General Security, to include ISSO Compliance

All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The Contractor shall conform to all security policies contained in the Security Policies and Procedures documentation. All services provided under this BPA must be compliant with Information Security Policy, identified in MD4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook.

12 SPECIAL CONSIDERATIONS

12.1 Issue and Risk Management Procedure

The following general procedure shall be used to manage project issues and risks:

- Identify and document
- Assess impact and prioritize
- Assign responsibility
- Monitor and report progress
- Communicate issue resolution

A mutually agreed issue escalation process shall be defined at the outset of execution for each Task Order during the kick-off meeting.

12.2 Qualification and Training

The Contractor shall maintain an appropriate level of technical competence in its areas of responsibility.

In addition to the Labor Categories identified in each Task Order, the Government requires Contractor personnel to have experience / knowledge using various office automation tools to include but not limited to Microsoft Office, SharePoint, and Dimensions.

12.3 Safeguarding Information

Contractors must control and safeguard FOUO information in accordance with DHS Directive (MD 11042.1) Safeguarding Sensitive but Unclassified (For Official Use Only) Information" dated January 6, 2005. DHS Contractors must sign a special Non-Disclosure Agreement before receiving access to FOUO information. Contractors with questions on handling DHS FOUO must contact DHS Office of Security (OS) Administrative Security Division (ASD) at (202) 447-5341.

Access to information FOUO and above is restricted to Government facilities only as directed by the contract task monitor (TM).

Contractors must adhere to Operational Security requirements as directed by the TMs and DHS directives.

- "All services provided under this BPA and subsequent Task Orders must be compliant with DHS Information Security Policy, identified in MD4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook."
- “All contract personnel should orient themselves with the CBP Security Policy and Procedures Handbook (HB1400-02B), August 13, 2009, Volume IV, Chapter 13, Safeguarding Sensitive But Unclassified (For Official Use Only) Information.”

12.4 Non-Disclosure of Information

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of the BPA and subsequent Task Orders and will not be divulged or made known in any manner to any persons except as may be necessary in the performance of the Task Order. The Contractor will be required to sign Non-Disclosure statements.

12.5 Other Direct Costs

There are no Other Direct Costs, other than travel, anticipated.

12.6 Contractor Personnel Duties

Provide qualified personnel to perform the work required.

- Supervision of personnel in the performance of their duties
- Providing instructions to Contractor employees to ensure that work progresses on schedule to meet any required deadlines and any accuracy requirements
- Coordination with COR, TM or designee in the assignment and prioritization of requested work
- Assurance that all deliverables are submitted as required

- When determined to be appropriate, Contractor employees may be required to execute a non-disclosure agreement as a condition to access of sensitive but unclassified information.

12.7 Key Personnel

Key personnel will be identified in the individual Task Orders and are considered essential to the work being performed.

12.8 Work Hours

Work hours will be as stated in the Task Order.

12.9 Contractor Employee Conduct

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance and integrity, and must be responsible for their employees' performance or the quality of their services.

12.10 Holidays and Administrative Leave

U. S. Customs and Border Protection (CBP) personnel observe the following days as holidays:

- New Year's Day
- Martin Luther King's Birthday
- Presidents Day
- Memorial Day
- Independence Day
- Labor Day
- Veterans Day
- Columbus Day
- Thanksgiving Day
- Christmas Day

Note: When a holiday falls on a non-workday – Saturday or Sunday – the holiday usually is observed on Monday (if the holiday falls on Sunday) or Friday (if the holiday falls on Saturday).

Any other day designated by Federal statute, by Executive Order or by the President's proclamation.

In the event CBP grants administrative leave to its Government employees, on-site Contractor personnel shall also be dismissed if the site is being closed. In each instance when the site is closed to Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances, the Contractor will direct its staff in accordance and OPM Operating Status for the Washington, DC area available by calling (202) 606-1900 or at http://www.opm.gov/Operating_Status_Schedules

Note: For those teams deemed 24x7x365, Federal Holidays do not apply. Contractor shall continue to maintain 24x7x365 staffing.

12.11 Travel

Travel may be required as identified in each Task Order. Travel will be performed in accordance with the Federal Travel Regulations (FTR). The COR/TM will identify travel requirements on a case by case basis. The COR/TM will approve all travel requests. Any travel must be in accordance with the Federal Travel Regulations (for travel in 48 contiguous states), the Joint Travel Regulations, DoD Civilian Personnel, Volume 2 Appendix A (for travel to Alaska, Hawaii, Puerto Rico, and U.S. territories and possessions), and if required, the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, “Maximum Travel Per Diem Allowances for Foreign Areas” (for travel not covered in the Federal Travel Regulations or Joint Travel Regulations).

Contractor personnel working at a government site will not be paid local travel costs when traveling to or from the work site. Other local travel costs may be allowed if requested in advance by the Contractor and with written consent from the COR/TM.

12.12 Task Order Administration

Notwithstanding the Contractor’s responsibility for management during performance, the administration of all Task Orders will require some coordination between the CBP and the Contractor. The CO will appoint a COR to assure orderly performance of the tasks and provide technical direction. The COR is:

(b) (6) [redacted]

On-site Task Monitors (OTM), unless otherwise stated in the Task Order, are:

(b) (6) [redacted]

(b) (6) [redacted]

The types of actions within the purview of the COR's authority are to assure that the Contractor performs the technical requirements of the contract; to perform or cause to be performed inspections necessary in connection with performance of the contract; to maintain both written and oral communications with the Contractor concerning the aspects of the contract within his/her purview; to issue interpretations of technical requirements; to monitor the Contractor's performance under the Task Order and notify the Contractor and CO of any deficiencies observed; and to coordinate Government-Furnished Property or Data availability and provide for site entry of Contractor personnel if required.

The COR will provide no supervision to Contractor personnel. The COR is not empowered to make any commitments or changes which affect the Task Order price or other terms and conditions. Any such proposed changes must be brought to the immediate attention of the CO for action. The acceptance of any changes by the Contractor without specific approval and written consent of the CO shall be at the Contractor's risk.

The types of actions within the purview of the TM authority are at the day to day tasking and work approval level.

12.13 Invoice Instructions

Invoices must separately identify costs for each Task Order including modifications. See BPA for additional invoice instructions.

12.14 Invoice Submission Method

See BPA for invoice submission method.

12.15 Invoice Detail

- See BPA for required invoice detail.

12.16 Detail required for Travel (per individual trip) if applicable in the Task Order:

- Date (start and end) for travel
- Task Order Number
- Travel description
- Travel breakdown (per diem, airfare, care rental, mileage, etc.)
- Copy of COR documentation approving the travel
- Total price for travel, by trip and total for all travel

ADDENDUM A: ACRONYM LISTING

Acronym	**Definition**
BI	Background Investigation
BOM	Bill of Materials
CBP	U.S. Customs and Border Protection
CFR	Code of Federal Regulations
CM	Configuration Management
CO	Contracting Officer
CONUS	Continental United States (Lower 48 states)
COR	Contracting Officer’s Representative
COTS	Commercial Off-the-Shelf
DAA	Decision Approval Authority
DCN	DHS Core Network
DHS	Department of Homeland Security
DOD	Department of Defense
DROC	Disaster Recovery Operation Center
EA	Enterprise Architecture
EDMO	Enterprise Data Management Office
EFT	Electronic Funds Transfer
EVM	Earned Value Management
EVMS	Earned Value Measurement System
FISMA	Federal Information Security Management Act
FMG	Financial Management Group
GOTS	Government of the Shelf
HLS	Homeland Security
HSDN	Homeland Security Data Network
IP	Internet Protocol
ISA	Interconnection Security Agreement
IT	Information Technology
LAN	Local Area Network
MAN	Metropolitan Area Network
MD	Management Directive
MNS	Managed Network Service
MOUs	Memorandum of Understanding(s)
MPLS	Multiprotocol Label Switching
MSP	Managed Service Provider
NCC	Network Communication Center
NDC	National Data Center
NLECC	National Law Enforcement Communications Center
NMT	Network Management Team
NOC	Network Operations Center
NSO	Network Security Operations
OAST	Office on Accessible Systems and Technology

OF	Office of Finance
OIs	Operating Instructions
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OneNet	DHS Single Network Project
OTM	The On-Site Task Manager
PE	Provider Edge
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestone
POP	Points of Presence
PR	Purchase Requisition
QoS	Quality of Service
SCI	Sensitive Compartmented Information
SLA	Service Level Agreements
SLO	Service Level Objectives
SOC	Security Operations Center
SOPs	Standard Operating Procedures
SOW	Statement of Work
TPOCs	Technical Point of Contact(s)
TRM	Technical Reference model
TTPs	Tactics Techniques Procedures
TTY	Teletypewriter of Teletype
VPN	Virtual Private Networking
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing
WAN	Wide Area Network

ADDENDUM B: TERMS AND CONDITIONS REFERENCE

EA (Enterprise Architecture) Compliance
The Offeror shall ensure that the design conforms to the DHS Homeland Security (HLS) and CBP EA, and all DHS and CBP policies and guidelines as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA) such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture Technical Framework.

The Contractorshall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model as described in their respective EAs. Models will be submitted using Business Process Modeling Notation (BPMN) version 2.0 and the CBP Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data exchange formats and semantics shall be in conformance with the National Information Exchange Model (NIEM), version 2.0. Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

The Contractor shall maintain close coordination with the CBP Enterprise Architecture Branch (EAB) and utilize the Central Enterprise Architecture Repository (CEAR), for capturing performance measures, business processes, application designs, technical infrastructure designs, and other related designs for the project. The Contractor shall develop performance indicators and ensure appropriate mapping to the Performance Reference Model (PRM); develop business process flows and ensure appropriate mapping to CBP Lines of Business and Business Reference Model (BRM); develop application models capturing system components, subsystems, and information exchanges between the system in development and other systems and ensure appropriate mapping of the system under development to Service Component Reference Model (SRM) and the Technical Reference Model (TRM); develop data models and data exchanges that align to the Data Reference Model (DRM) and develop models of technical infrastructure that will be used to support the systems under development.

All IT hardware and software shall comply with the DHS and CBP TRMs. The Contractor shall use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP TRM/Standards Profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal technology insertion process which includes a trade study with no less than four alternatives, one of which shall reflect the status quo and one shall reflect multi-agency collaboration. The DHS/CBP TRM/Standards Profile will be updated as technology insertions are accomplished.

Description information forall data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS DRM and Enterprise Architecture Information Repository. Submittal shall be through the CBP Data Engineering Branch and CBP EAB.

All developed solutions shall be compliant with the HLS and CBP EA.
Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

In compliance with Office of Management and Budget (OMB) mandates, all network hardware provided under the scope of this Statement of Work and associated Task Orders shall be IPv6 compatible without modification, upgrade, or replacement.

Accessibility Requirements (Section 508 Compliance)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.25 Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and determination will be made in accordance with DHSMD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHSMD 4010.2.

All tasks for testing of functional and/or technical requirements shall include specific testing for Section 508 compliance, and shall use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

ISO (Information Security) Compliance

(b) (7)(E)

[redacted]

[redacted]

System Security Documentation Appropriate for the SELC Status

Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SELC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS information system. System owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

Monitoring/Reviewing Contractor Security Requirements Clause

Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer,Office of Inspector General, the CBP Chief Information Security Officer, authorized Contracting Officer's Technical Representative (COR), and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how Contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering Contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the Contractor except as specified in the Task Order.